UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417	7632

7590 03/24/2005

Orange & Chari
66 Wellington Street West, Suite 4900
P.O. Box 190
Toronto, ON M5K 1H6
CANADA

EXAMINER	
GELAGAY, SHEWAYE	

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 03/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/025,924	VANSTONE ET AL.	
	Examiner	Art Unit	
	Shewaye Gelagay	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *December 26, 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 December 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-14 have been examined.

Oath/Declaration

2. The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by application number and filing date is required. See MPEP §§ 602.01 and 602.02.

The oath or declaration is defective because: It is not signed by the inventors.

Drawings

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: On Page 4, line 31 and Page 5, line 19, "a system 10". Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner,

the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

4. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: On Page 4, line 33, "a communication link 16". Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-2 and 4-5 are rejected under 35 U.S.C. 102(b) as being anticipated by Schneier "Applied Cryptography", (Pages 483-490).

As per claim 1:

Schneier teaches a method of generating a key over a group of order q, said method including the steps of:

generating a seed value from a random number generator; (Page 487, line 11; Page 489, lines 15-16)

performing a hash function on said seed number to provide an output; (Page 487, lines 7-8; Page 489, lines 17-18)

determining whether said output is less than said prime number q; (Page 487, line 11; ...k less than q)

accepting said output for use as a key if the value thereof is less than said prime number q; (Page 487, lines 12-15) and

rejecting said output as a key if said value is not less than said order q. (Page 487, line 11)

As per claim 2:

Schneier teaches all the subject matter as discussed above. In addition, Schneier further discloses a method wherein another seed value is generated by said random number generator if said output is rejected. (Page 487, line 11; Page 489, line 22)

As per claim 4:

Schneier teaches all the subject matter as discussed above. In addition, Schneier further discloses a method wherein said key is used for generation of a public key. (Page 487, lines 8-15; Page 488, line 3-8)

As per claim 5:

Schneier teaches all the subject matter as discussed above. In addition, Schneier further discloses a method wherein said order q is prime number represented by a bit string of predetermined length l. (Page 487, line 1 and Page 488, line 5)

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

8. Claims 7-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography", (Pages 483-490) in view of Backal United States Letter Patent Number 6,219,421.

As per claim 7:

Schneier teaches all the subject matter as discussed above. Schneier does not explicitly disclose a method wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key.

Backal in analogous art, however, disclose a method wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key. (Col. 5, lines 61-67)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner to include a method of wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Backal (Col. 1, lines 50-51) in order to provide an exceptional degree of security. This way, the keys generated using the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document.

As per claim 8:

Schenier and Backal teach all the subject matter as discussed above. In addition, Backal further discloses a method wherein said step of incrementing includes a further step of adding a particular value to said seed value. (Col. 5, lines 61-67)

As per claim 9:

Schneier teaches a method of generating a key over a group of order q, said method including the steps of:

generating a seed value from a random number generator; (Page 487, line 11; Page 489, lines 15-16)

performing a hash function on said seed number to provide a first output; (Page 487, lines 7-8; Page 489, lines 17-18)

accepting said new output as a key k if said new output has a value less than order q; (Page 487, line 11; ...k less than q) and

rejecting said new output as a key if said new output has a value less than order q . (Page 487, line 11)

Schneier does not explicitly disclose a method of incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order q.

Backal in analogous art, however, disclose a method of

incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; (Col. 5, lines 61-67) and

combining said first output and second output to produce a new output; determining whether said new output has a value less than said order q; (Col. 5, lines 54-60)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner to include a method of incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order q. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Backal (Col. 1, lines 50-51) in order to provide an exceptional degree of security. This way, the keys generated using the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document.

As per claim 10:

Schenier and Backal teach all the subject matter as discussed above. In addition, Schenier further discloses a method wherein upon rejection of said new output a new seed value is generated by said random number generator. (Page 487, line 11; Page 489, line 22)

As per claim 11:

Schenier and Backal teach all the subject matter as discussed above. In addition, Backal further discloses a method wherein upon rejection of said new output said seed value is incremented by a predetermined function and revised values for said first output and said second output are obtained. (Col. 5, lines 61-67)

As per claim 12:

Schenier and Backal teach all the subject matter as discussed above. In addition, Schenier further discloses a method wherein a bit string greater than a predetermined length l is obtained and an l bit string selected therefrom for comparison with said order q. (Page 487, line 1 and Page 488, line 5)

As per claim 13:

Schenier and Backal teach all the subject matter as discussed above. In addition, Schenier further discloses a method wherein upon rejection of said bit string of predetermined length l, a further l bit string is selected. (Page 487, line 1 and Page 488, line 5)

9. Claims 3 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography", (Pages 483-490) in view of Nel et al. "Generatiion of Keys for use with the Digital Signature Standard (DSS)" (Pages 6-10).

As per claim 3:

Schneier teaches all the subject matter as discussed above. Both references do not explicitly disclose a method wherein the step of accepting said output as a key includes a further step of storing said key.

Nel et al. in analogous art, however, discloses a method wherein the step of accepting said output as a key includes a further step of storing said key. (Page 10, Col. 1, lines 3-4)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner to include a method wherein the step of accepting said output as a key includes a further step of storing said key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so in order to be able to reuse the key and also to perform auditing on the key generation process.

As per claim 6:

Schneier teaches all the subject matter as discussed above. Schneier does not explicitly disclose a method wherein said output from said hash function is a bit string of predetermined length l.

Nel et al. in analogous art, however, discloses a method wherein said output from said hash function is a bit string of predetermined length l. (Page 8, Col. 2, lines 8-11)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner to include a method wherein said output from said hash function is a bit string of predetermined length l. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Nel

et al. (Page 8, Col. 2, lines 6-7) in order to prevent constructing a message which will yield a known value of message digest.

10. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography", (Pages 483-490) in view of Backal United States Letter Patent Number 6,219,421 and further in view of Nel et al. "Generatiion of Keys for use with the Digital Signature Standard (DSS)" (Pages 6-10).

As per claim 14:

Schenier and Backal teach all the subject matter as discussed above. Both references do not explicitly disclose method wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length l.

Nel et al. in analogous art, however, discloses a method wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length l. (Page 8, Col. 2, lines 8-11)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner to include a method wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length l. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Nel et al. (Page 8, Col. 2, lines 6-7) in order to prevent constructing a message which will yield a known value of message digest.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 571-272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay
Exminer
Art Unit 2133

03/04/05

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100